Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1606 02/07/14

~ NYPD Uses Google Glass ~ People Are Talking! ~ New YouTube Exec!
~ French Court to Google ~ EA Responds to Critics ~ Tablet Kill Switch?
~ Naughty Dog Moves On! ~ Edit Look Back Movie! ~ Jerks Online, Why?

-* Hacked in Sochi in Minutes! *-
-* Source of Target Hack: HVAC Company *-
-* Cybersecurity Expert to NBC: 100% Fraud Tale *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

More "weather" here in the Northeast! It appears that we’re in the middle of a long, cold, and snow-filled winter this year. Earlier this week, we had to dig out of about a new foot of snow. That was shortly after getting a couple of inches (to whet our appetite?) a few days earlier. I don’t think that Spring is going to get here any time quickly!

The 2014 Winter Olympics is starting tonight; and I’ll probably watch a little of it later this evening. There are a number of events that I enjoy, so I’m looking forward to them. Here’s hoping that the games take place without incident!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Naughty Dog Brainstorming The Last of Us 2
""""""""""""""""""""""""""""""" EA Responds To Dungeon Keeper s Criticisms!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Naughty Dog Brainstorming The Last of Us 2, Other Games

A day after cleaning up at the 2014 DICE Awards for its work on The Last of Us, developer Naughty Dog has revealed that it is already thinking about a sequel to the Game of the Year as well as other, brand new IPs.

Speaking with Eurogamer, writer and creative director at Naughty Dog Neil

Druckmann stated that while it s time to let the batteries recharge after working on the game for four years, his team has been working on ideas for the future.

 We have started brainstorming some stuff. To be honest, some of them are sequel ideas, and some of them are brand new IP   we ve spent the last few weeks brainstorming new IP, he said. So we have to get some good steps and see

 It s kind of like how we approached Left Behind. Can we tell people a story that s really worth telling, and that s not repeating itself? And if we can t, where can we get inspired   what is something that s really going to challenge us, and push storytelling in this medium forward?

Naughty Dog is currently working on a brand new game in the Uncharted series for the PlayStation 4, but it s only a matter of time before news comes out of what the company s next big project will be.

EA Responds To Dungeon Keeper s Criticisms

Dungeon Keeper was a game originally developed back in 1997 by Peter Molyneux and was designed to be a game in which you play as the bad guy, where you build a dungeon in an attempt to keep invading heroes out. We re sure many gamers have spent countless hours on the original game back in the day which is why many were excited when EA released a remake of the game onto mobile devices. Unfortunately it looks like EA might have taken the free-to-play model a bit too far, leading to many criticizing the company for it.

EA Mythic senior producer Jeff Skalski has since responded to those criticism (via Tab Times). I think any time you re-make anything that is much beloved and has a great sense of nostalgia for people be it a game, a movie, or whatever people are going to be very protective of it. They have fond memories of it. We, as gamers, have our own fond memories of it. Our intention with the mobile version was to give as many people as possible a taste of that original Dungeon Keeper experience, and for some people, that s not the way they want to re-visit the franchise.

For those who have yet to play the game, EA has been very aggressive in getting players to spend real money, such as prompting gamers in-game to spend more money in order to get certain tasks done faster, which many gamers felt was a bit unfair and to a certain extent, a bit spammy too. On the flipside Skalski claims that there are many who are still enjoying the game, Obviously, this is counter to some of the angry reactions we ve seen around the Internet, so we re still trying to look at all of these data points.

=~=~=~=

Hacked in Sochi in Minutes: Russian Cyberspace Full of Risks

Privacy in all forms is a very rare commodity at the Sochi Olympics, according to a report from NBC News.

Athletes, journalists and fans are reportedly seeing their cell phones, computers and tablets hacked. The report, by NBC News' Richard Engel, demonstrates how quickly the hackings occur.

In an experiment conducted with the help of an American computer security expert, Engel created a fake online identity with fake contact lists, phony names and addresses. It's called baiting the hook.

In Russia, the pair fired up two new laptop computers loaded with Engel's fake profile to see how long it would take hackers to do their business.

They didn't have to wait long in less than a minute, Engel received what appeared to be a custom email welcoming him to Sochi and asking him to click on a link for information he might find useful. After clicking, Engel said, his computer was "hijacked."

It was the same scenario with Engel's cell phone. "Malicious software hijacked our phone before we even finished our coffee, stealing my information and giving hackers the option to tap and record my phone calls," Engel said.

For those traveling to Sochi for the Games, Engel recommends not bringing phones or laptops if at all possible. If you can't be without a connection, delete any sensitive information from devices before logging on. And as with "phishing" scams, don't click on anything in an email or a Web page that takes you to an external link, as Web sites that appear to belong to banks or other "secure" third parties can be easily faked.

Hackers who hail from Russia are known to be among the world's most skilled. The 2013 hacks of retailers Target and Neiman Marcus were traced back to a Russian teenager. However, according to Bloomberg, "China accounted for 41 percent of the world's attack traffic" during the fourth quarter of 2012.

Cybersecurity Expert Accuses NBC of 100% Fraudulent Hacking Story, NBC Fires B ack

Earlier this week, NBC s Richard Engel filed a report warning travelers to Sochi about the danger of getting hacked, but one cybersecurity expert took serious issue with the story, which he described on his blog as 100% fraudulent.

In the report, Engel brought some brand-new laptops and a new phone just to test how secure people s devices would be in Sochi, and he concluded that he was hacked almost immediately. But Robert Graham pointed out a few reasons why all is not as it seems.

1. They aren t in Sochi, but in Moscow, 1007 miles away.

2. The hack happens because of the websites they visit (Olympic themed websites), not their physical location. The results would ve been the same in America.

3. The phone didn t get hacked; Richard Engel initiated the download of a hostile Android app onto his phone.

4. and in order to download the Android app, Engel had to disable a lock that prevents such downloads something few users do [update].

He explained that the real issue is geolocation, meaning that from inside Russia you ll see more dodgy Russian sites in the results, which can be easily disabled in the settings. Graham concluded, The only thing that can be confirmed by the story is don t let Richard Engel borrow your phone.

NBC fired back against his criticisms in a point-by-point statement to Business Insider, saying that it was completely clear Engel was in Moscow and that the entire story was supposed to be about alerting the layman.

NBC said the story was designed to show how easily a non-expert could fall victim to a hack. Just like any regular user, Richard went online, searched sites and was very quickly targeted and received a tailored fake message designed to trick him into downloading the software.

Target Hackers Broke in Via HVAC Company

Last week, Target told reporters at The Wall Street Journal and Reuters that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer s network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the U.S. Secret Service visited his company s offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President Daniel Mitsch declined to answer questions about the visit. According to the company s homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe s, Whole Foods and BJ s Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

Target spokeswoman Molly Snyder said the company had no additional information to share, citing a very active and ongoing investigation.

It s not immediately clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target s payment system network. But according to a cybersecurity expert at a large retailer who asked not to be named because he did not have permission to speak on the record, it is common for large retail operations to have a team that routinely monitors energy consumption and

temperatures in stores to save on costs (particularly at night) and to alert store managers if temperatures in the stores fluctuate outside of an acceptable range that could prevent customers from shopping at the store.

To support this solution, vendors need to be able to remote into the system in order to do maintenance (updates, patches, etc.) or to troubleshoot glitches and connectivity issues with the software, the source said. This feeds into the topic of cost savings, with so many solutions in a given organization. And to save on head count, it is sometimes beneficial to allow a vendor to support versus train or hire extra people.

Investigators also shared additional details about the timeline of the breach and how the attackers moved stolen data off of Target s network.

Sources said that between Nov. 15 and Nov. 28 (Thanksgiving and the day before Black Friday), the attackers succeeded in uploading their card-stealing malicious software to a small number of cash registers within Target stores.

Those same sources said the attackers used this time to test that their point-of-sale malware was working as designed.

By the end of the month just two days later the intruders had pushed their malware to a majority of Target s point-of-sale devices, and were actively collecting card records from live customer transactions, investigators told this reporter. Target has said that the breach exposed approximately 40 million debit and credit card accounts between Nov. 27 and Dec. 15, 2013.

While some reports on the Target breach said the stolen card data was offloaded via FTP communications to a location in Russia, sources close to the case say much of the purloined financial information was transmitted to several drop locations.

These were essentially compromised computers in the United States and elsewhere that were used to house the stolen data and that could be safely accessed by the suspected perpetrators in Eastern Europe and Russia.

For example, card data stolen from Target s network was stashed on hacked computer servers belonging to a business in Miami, while another drop server resided in Brazil.

Investigators say the United States is currently requesting mutual legal assistance from Brazilian authorities to gain access to the Target data on the server there.

It remains unclear when the dust settles from this investigation whether Target will be liable for failing to adhere to payment card industry (PCI) security standards, violations that can come with hefty fines.

Avivah Litan, a fraud analyst with Gartner Inc., said that although the current PCI standard (PDF) does not require organizations to maintain separate networks for payment and non-payment operations, it does require merchants to incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties including vendor access for support or maintenance.

In any case, Litan estimates that Target could be facing losses of up to $420 million as a result of this breach, including reimbursement associated with banks recovering the costs of reissuing millions of cards; fines from the card brands for PCI non-compliance; and direct Target customer service costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach.

Litan notes these estimates do not take into account the amounts Target will spend in the short run implementing technology at their checkout counters to accept more secure chip-and-PIN credit and debit cards. In testimony before lawmakers on Capitol Hill yesterday, Target s executive vice president and chief financial officer said upgrading the retailer s systems to handle chip-and-PIN could cost $100 million.

Target may be able to cover some of those costs through a mesh network of business insurance claims. According to a Jan. 19 story at businessinsurance.com, Target has at least $100 million of cyber insurance and $65 million of directors and officers liability coverage.

Update, Feb. 6, 3:33 p.m. ET: Fazio Mechanical Services just issued an official statement through a PR company, stating that its data connection with Target was exclusively for electronic billing, contract submission and project management. Their entire statement is below:

Fazio Mechanical Services, Inc. places paramount importance on assuring the security of confidential customer data and information. While we cannot comment on the on-going federal investigation into the technical causes of the breach, we want to clarify important facts relating to this matter:

- Fazio Mechanical does not perform remote monitoring of or control of heating, cooling and refrigeration systems for Target.

- Our data connection with Target was exclusively for electronic billing, contract submission and project management, and Target is the only customer for whom we manage these processes on a remote basis. No other customers have been affected by the breach.

- Our IT system and security measures are in full compliance with industry practices.

Like Target, we are a victim of a sophisticated cyber attack operation. We are fully cooperating with the Secret Service and Target to identify the possible cause of the breach and to help create proactive initiatives that will further enhance the security of client/vendor connections making them less vulnerable to future breaches.

French Court Orders Google To Display Fine for Privacy Breach

Google will have to display on its French search page a notice saying it has been fined by the local data-protection watchdog over how user information is tracked and stored, France’s top administrative court ruled on Friday.

The U.S. search engine said it would comply with the order but would keep fighting the 150,000-euro ($204,000) fine issued last month by privacy watchdog CNIL.

CNIL has objected to Google’s method of combining data collected on individual users across services such as YouTube, Gmail and social network Google+. The move towards broad storage was introduced by Google in March 2012 and combined 60 privacy policies into one, giving users no means to opt out.

The web giant appealed the CNIL’s fine last month as well as the order to post a notice of the sanction on its google.fr homepage for 48 hours. Google specifically asked the Conseil d’Etat, France’s top administrative court, to suspend that order while it re-examines the case.

On Friday, the Conseil d’Etat ruled that there was not enough urgency nor proof of damage to Google’s reputation to warrant such a suspension. This means Google will have to post the CNIL’s decision on its French homepage even while it keeps fighting it in court.

"We’ve engaged fully with the CNIL throughout this process to explain our privacy policy and how it allows us to create simpler, more effective services," a Google spokesman said in an e-mailed statement.

"We will comply with the order to post the notice, but we’ll also continue with our appeal before the Conseil d’Etat."

Spain, Britain, Germany, Italy and the Netherlands have also opened similar cases against Google, arguing that its privacy policy breached local rules protecting consumers on how their personal data is processed and stored.

Facebook Now Lets You Edit Your Look Back Movie

Earlier this week, we learned that Facebook would soon let you edit the automatically-generated Look Back videos the company had made to celebrate Facebook s 10th anniversary.

Sure enough: they just launched the editor.

Almost immediately after launch, many users were complaining about the photos that Facebook auto-selected. Some had too many photos of their exes. Some had sad photos that they d rather not remember as a milestone. One of my friends Look Backs prominently featured a picture of a rock, sans explanation or commentary.

A quick visit to the Facebook Lookback page now shows a shiny new edit button.

The editor might not be quite as feature-rich as some might have hoped; you can t choose ANY Facebook photo to replace those that you don t like you can just select from a wider array of pre-picked photos/status updates.

How To Edit Your Look Back:

- Go to the Facebook Lookback page
- Hit the edit button
- Pick your new photos/posts from the pre-populated selections
- Hit the Update button at the top of the page

Wait a few minutes for Facebook to generate your new video.

It s unclear if the edit feature has been launched to all users, or if it s being rolled out over time. We ve checked on around a dozen accounts now, however, and each one had the new button.

Google Taps Longtime Executive Wojcicki To Head YouTube

Google Inc executive Susan Wojcicki has been appointed new head of the company’s YouTube video business, a source familiar with the matter told Reuters.

The move, in which Wojcicki will replace Salar Kamangar, represents the latest change to Google’s top properties by Chief Executive Larry Page and comes as Google is striving to turn the popular video portal into a bigger money-maker.

"It’s one of the biggest traffic sources on the Internet, so it makes sense to want to try to monetize the best they can," said Needham & Co. analyst Kerry Rice.

Google does not disclose YouTube’s financial results, though analysts believe the website generates several billions of dollars in annual revenue from video ads and other promotions.

Wojcicki who is a member of Page’s inner circle of top managers known as the "L" Team, was most recently senior vice president of Ads and Commerce. She shared the title with Sridhar Ramaswamy, another Google executive.

Wojcicki’s new job is effective immediately, according to the source. It was not immediately clear what Kamangar would do. A report in the tech blog The Information, which first reported news of the change, said that Kamangar was expected to remain at Google, perhaps playing a greater role in Google’s in-house venture capital arm.

YouTube, the world’s No. 1 video website, is moving to add professional-grade video programs to the vast archive of amateur, home-shot videos as it seeks to attract a bigger slice of the estimated $70 billion in spending on U.S. television ads.

"Like Salar, Susan has a healthy disregard for the impossible and is excited about improving YouTube in ways that people will love," Page said in a statement.

The change at YouTube comes nearly a year after Google appointed Sundar Pichai to lead its Android mobile software group, taking over from Andy Rubin, who is now spearheading a secretive group within Google that is developing robots.

Wojcicki has been with Google from its earliest days. Page and co-founder Sergey Brin set up shop in the garage of Wojcicki’s Menlo Park, California home in September 1998, around the time they incorporated the company.

NYPD To Fight Crime With Google Glass

The NYPD is taking a page out of the RoboCop playbook outfitting cops with Google Glass so a suspect s life story can flash right before their eyes, law enforcement sources told The Post.

Department bosses bought a few pairs of the futuristic eyewear and are beta testing them with the hopes of using them out in the field.

’It would be like the Terminator. You walk past somebody and you get his info.’

- Law enforcement source

It s in the early stages, a source said of the NYPD s use of the specs. A handful of people are testing it out.

The high-tech glasses which integrate a computerized interface into the wearer s field of vision could allow cops to instantly see a suspect s arrest record, mugshot and other key information.

If it works, it could be very beneficial for a cop on patrol who walks into a building with these glasses on, the source said.

It would be like the Terminator. You walk past somebody and you get his pedigree info if he s wanted for a warrant right on your eye screen.

You can identify the bad guys immediately within seconds.

In addition to providing cops with instant internet access, Google Glass could also be used to record audio and video of interactions with suspects and other members of the public.

That would enhance the safety of officers, the source said. It s a win win for cops and the public.

San Francisco Senator Wants to Place Kill Switches on Smartphones, Tablets

A new California bill could force mobile smartphone and tablet makers to place a "kill switch" on their devices in order to prevent theft.

According to The New York Times, Sen. Mark Leno (D-San Francisco) is expected to introduce the bill Friday, which would require all smartphones and tablets sold in California to have a kill switch.

Having a feature like this would make the smartphone or tablet unusable if it were stolen. In turn, Leno hopes that this will curb robberies of mobile devices, since they would be more difficult to sell that way.

The bill, which is sponsored by George Gascón - San Francisco s district attorney - would make it so phones sold in California on or after Jan. 1, 2015 are required to have kill switches. Those who fail to do so could face fines of up to $2,500 for each device sold.

With robberies of smartphones reaching an all-time high, California cannot continue to stand by when a solution to the problem is readily

available, said Leno. Today we are officially stepping in and requiring the cellphone industry to take the necessary steps to curb violent smartphone thefts and protect the safety of the very consumers they rely upon to support their businesses.

However, CTIA - the industry trade group that represents mobile carriers like AT&T, Verizon Wireless and T-Mobile - said a kill switch isn't the answer because hackers could take control of the feature and disable other phones. Also, it noted that the original owners wouldn't be able to reactivate their phone if they manage to find it.

While solutions like a nationwide database of phones reported stolen has been put in place, theft rates are still high. In San Francisco alone, 2,400 cellphones were stolen last year, which represents a 23 percent increase from 2012.

The city has especially tried to tackle iPhone theft, as the Apple smartphone remains a popular target. Last April, San Francisco Police Capt. Joe Garrity described how the cross at Seventh and Market Street in downtown San Francisco is the main place for selling/buying stolen iPhones. The report noted that about 48 percent of San Francisco residents use an iPhone.

Why Are People Such Jerks Online?

When s the last time a total stranger walked up to you at a party and just started berating you?

 You should be ashamed of yourself. You should be fired for being such a spineless shill. Maybe they ll replace you with someone who has a clue.

I m guessing that no stranger has ever spoken to you like that. Nobody except the tragically unstable would open a conversation with you, in person, with that kind of intensity.

But online, this happens all the time. If you re a writer, you get email like that routinely. Even if you re not a writer, you see that sort of language in the cesspools I mean the comments areas of many websites.

It s a problem. The Web has the potential to eliminate our differences in geography, social class and demographic breakdown. It could be humanity s best hope for freedom of speech. It could be an amazing, centralized forum for useful discussion, solving problems, moving forward.

Instead, all too often, it s a place for the anonymous and insecure to take potshots. It seems to be a global incarnation of that old, sad rule: If you can t feel good about yourself, at least you can make somebody else feel worse.

For many years, I ve pondered why the Internet turns people into walking toxic spewers people who, in real life, might be perfectly nice. (I ve also wondered if people ever heap hatred unknowingly at people they actually know. Kind of like when you honk angrily at another driver, and then realize, as he seems to follow you all the way home, that you ve just been a jerk to your own neighbor.)

For most of those years, I had these theories:

On the Internet, you re anonymous. There are no social repercussions for having a tantrum. Nobody knows who you are.

There are thousands of other voices all around you. So you feel the need to shout because, deep inside, you worry that you won t be heard.

As I ve often said, technology has become a surprisingly politicized field. A phone or tablet has become a fashion statement a lifestyle choice and it s always open season for criticizing people who ve made different choices. (See: Mac vs. Windows, iPhone vs. Android, iPhone vs. Samsung, and so on.)

There might be a youth factor at play. Today s youngsters spend much less time in face-to-face social interactions than their parents did. So they may not be very good at being civil because they ve had less practice being civil. (What will happen when they seek a job? Or a spouse?)

Lately, though, I ve collected two new data points on this question. To me, they shed more light on the Why are people such nasties online? question.

First data point: So far, it s much better now that I m at Yahoo.

During the 13 years I wrote for The New York Times, the nastygrams amounted to about 25 percent of the reader email. Yahoo Tech has only been open for a month, but so far, my readers email has been far more civil.

That s not to say that people aren t critical you, dear readers, have plenty of good suggestions for Yahoo Tech s improvement. But for some reason, you ve been surprisingly constructive about it.

Example: Hi David: The new site is entertaining and very informative. But I wanted to say that I am really tired of all the continuing CES stuff you are sort of running it in the ground. The event is over and the articles are stale. Otherwise, keep up the good work!

My correspondent is correct. We re working on it. But do you see how gracefully he made his suggestion? Do you see why he s much more likely to get action than if he d just fired off a nastygram?

So what s going on here? Why are Yahoo Tech s commenters much more civil than The New York Times commenters?

Is it that our site is so new, visitors are cutting us some slack?

Is it that leaving feedback requires some effort, so casual drive-by insults aren t worth making? (We re building a great new comments system so, for now, the only way to leave feedback on a Yahoo Tech story is to email the author.)

Or is it that The New York Times is considered an All-Powerful, Shining Obelisk of Power and is therefore a bigger target to tear down?

I think that s it. I think the higher your profile, the riper you are for potshots. When people post things online about co-workers or fellow school parents, they re much less horrible than when they say things about, say, members of Congress or Justin Bieber. At least I hope so.

Second data point: The following exchange, concerning this Ask Pogue

article:

Reader, dripping with sarcasm: Good Job not answering Tamara s question and instead answering an entirely different one. Kudos.

My reply: What do you mean?

Tamara asked: I m thinking home phone lines and cable subscriptions. Do you agree? What about books and newspapers?

I answered Tamara like this:

Everyone thinks cable TV is dying, since so many people have now cut the cord and watch TV exclusively on the Internet (from Netflix, Hulu and so on). But the cord-cutters add up to 1 million people a year just 1 percent of all U.S. cable subscriptions. Cable TV will not be going away in three to five years!

Home phone lines are also a lot less popular, thanks to cellphones and voice-over-Internet services like FaceTime and Skype. So maybe they ll fade away, too but in 20 years, not five.

In what way didn t I answer?

Reader: I apologize. I was definitely in a sour mood this afternoon and had no right to take it out on a perfect stranger. You did directly address the examples she provided.

Now, that s big of my reader to apologize. But here s the nutty part: That pattern goes on all the time!

I mean, hundreds of times over the years.

Reader: Nastygram. Me: Calm reply. Reader: Apology.

What the heck is going on?

My guess is that the reader never really expects a reply. She finds me guilty before the trial. Her thinking is: He s this almighty columnist who doesn t care what I think. What a jerk! So her initial email has resentment for being ignored built in before it s actually happened.

Then, when she gets a reply, she s a little embarrassed. Suddenly this is no longer an anonymous exchange, as in a comments section, but a personal exchange, as at a party. In that context, her initial volley seems inappropriate too heated, too intense.

It s a shame it has to be this way. It s a shame we can t start out civil, with the assumption that people care about our opinions. Maybe that kind of maturity comes with experience; I know for sure that I d never send a nastygram, even to someone with whom I heartily disagree, even to a big, famous person. (After all, I ve been on the receiving end.)

I don t really expect that anything will change. As long as you can hide behind anonymity online as long as we get secret pleasure from putting other people down as long as there are no repercussions for incivility nothing will change.

But maybe, just maybe, now that you, O Reader, have considered what makes

people nasty, you ll take that one moment to reword your comment before you send it. Life isn t long; let s do what we can to make it a pleasant ride.

=~=~=~=